國立交通大學應用數學系
離散專題演講公告

主講人：Prof. Clemens Heuberger

Alpen-Adria-Universitaet Klagenfurt (AAU)

講　題：Efficient Scalar Multiplication in Elliptic Curve Cryptography

時　間：105年9月26日(星期一) 下午2：00～3：00

地　點：(光復校區)科學一館213室

Abstract

Scalar multiplication is the key operation in public key cryptosystems implemented via elliptic (or hyperelliptic) curves. One strategy to implement it efficiently uses suitable digit expansions. Having a larger set of digits than strictly necessary introduces redundancy which can be used to minimize the number of expensive curve operations. Apart from binary expansions, expansions to complex bases are used; these correspond to efficient endomorphisms on the curve. We give a survey on these methods and their asymptotic analysis.

敬請公告　　歡迎參加

應用數學系　啟